ADVANCES IN MATHEMATICS 114, 189–196 (1995)

Generic Norms, II

N. JACOBSON

Department of Mathematics, Yale University, 10 Hillhouse Avenue, Box 2155, Yale Station, New Haven, Connecticut 06520

DEDICATED TO GEORGE SELIGMAN ON HIS 65TH BIRTHDAY

In this paper we define a generic norm in the Lie algebra $(1-K)A$ where A is central simple of even degree and K is an involution of orthogonal type in A. We apply this in the case of algebras of degree 4 to give a derivation based on generic norms from recent results of Knus, *et al.* ([7]) on the splitting of such algebras with involution.

1. GENERIC NORM IN LIE ALGEBRAS $(1-K)A$, K OF ORTHOGONAL TYPE

Let A be a finite-dimensional central simple associative algebra over an infinite field F such that $[A] \in \mathrm{Br}_2(F)$, the subgroup of the Brauer group of classes $[A]$ such that $[A]^2 = 1$. If the degree of A is odd we have the trivial situation in which $[A] = 1$. Hence we assume the degree of $A = n = 2m$, $m \geqslant 1$. A classical result of Albert [1] states that $[A] \in \mathrm{Br}_2(F)$ if and only if A has an involution over F. There are two types of such involutions, the *orthogonal type*, in which $(A, J)_{\bar{F}} \cong (M_n(\bar{F}), t)$ for $\bar{F}$ the algebraic closure of F where t is the transpose involution in $M_n(\bar{F})$, and the *sympletic type*, in which $(A, J)_{\bar{F}} \cong (M_n(\bar{F}), t_s)$ where t_s is the sympletic involution $a \rightsquigarrow s({}^t a)s^{-1}$, $s = \mathrm{diag}\{q, q, ..., q\}$, $q = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

We consider first an involution J of symplectic type in A. We have the special Jordan algebra $H(A, J) = (1+J)A$ in which we have defined the generic norm n_H and the generic adjoint $\#_H$ such that

$$a^{\#_H} a = n_H(a)\, 1 = a a^{\#_H} \tag{1}$$

([6]). Here n_H is a homogeneous polynomial function of degree m and $\#_H$ is a homogeneous polynomial map of degree $m-1$ in $H(A, J)$. These properties characterize n_H and $\#_H$ up to non-zero scalars since we have the following.

0001-8708/95 $12.00

607 114 2-2

PROPOSITION 1. *Let p_J be a polynomial map of $H(A, J)$ into itself of degree $(m-1)$ such that*

$$ap_J(a) = p_J(a)\, a \in F1, \qquad a \in H(A, J). \tag{2}$$

Then $p_J = \rho \#_H$, $\rho \in F^*$.

Proof. By (2), $a \to ap_J(a)$ is a polynomial function of degree m. Moreover, if $ap_J(a) \neq 0$ then a is invertible in $H(A, J)$ and hence $n_H(a) \neq 0$. Thus the set of zeros of n_H is contained in the set of zeros of xp_J. This carries over to the algebraic closure $\bar{F}$ of F. It follows from the irreducibility of n_H in $\bar{F}$ (since the Pfaffian is irreducible and $n_H(a) = \mathrm{Pf}(as)$) by the Hilbert Nullstellensatz that $n_H \mid xp_J$. Comparison of degrees shows that $xp_J = \rho n_H$, $\rho \in F^*$. Hence $ap_J(a) = \rho n_H(a) = \rho a a^{\#}$, $a \in H(A, J)$. Then $p_J(a) = \rho a^{\#}$ holds for $ap_J(a) \neq 0$ and hence holds for all a by Zariski density. ∎

The special Jordan algebra $H(A, J)$ contains 1 and $n_H(1) = 1$. We recall also that $\#_H$ satisfies the identity

$$a^{\#_H \#_H} (= (a^{\#_H})^{\#_H}) = n_H(a)^{m-2} a \tag{3}$$

([6]). This is called the *adjoint identity* for $\#_H$ which is called the *Jordan adjoint* in $H(A, J)$.

Now let K be an involution of orthogonal type in A. We can choose an involution J of symplectic type in A. Then $K = i_u J$ where $Ju = -u$ (i_u: $a \to uau^{-1}$ in A). Let $S(A, K) = (1-K)A$. This is a subalgebra of the Lie algebra A^- which is A with the Lie product $[ab] = ab - ba$. Then $a \in H(A, J)$ if and only if ua and $ua^{-1} \in S(A, K)$. Hence we have the bijective linear maps $a \to ua$ and $a \to au^{-1}$ of $H(A, J)$ onto $S(A, K)$ with inverses $b \to u^{-1}b$ and $b \to bu$, respectively. We now define a map p_K of $S(A, K)$ into itself by

$$p_K(b) = (u^{-1}b)^{\#_H} u^{-1}. \tag{4}$$

Then p_K is a polynomial map of degree $(m-1)$ of $S(A, K)$ into $S(A, K)$ since $\#_H$ is a polynomial map of degree $(m-1)$ of $H(A, J)$ into $H(A, J)$. We have

$$bp_K(b) = b(u^{-1}b)^{\#_H} u^{-1} = u(u^{-1}b)(u^{-1}b)^{\#_H} u^{-1} \in F1, \tag{5}$$

and similarly

$$p_K(b)\, b = bp_K(b). \tag{6}$$

We can now state the following.

THEOREM 1. *Let A be a central simple associative algebra of degree $n = 2m$, let K be an involution of orthogonal type in A, and let $S(A, K) = (1 - K)A$. Then there exists a polynomial function n_K of degree m on $S(A, K)$ and a polynomial map p_K of degree $(m-1)$ of $S(A, K)$ into itself such that*

$$bp_K(b) = n_K(b)1 = p_K(b)\,b, \qquad b \in S(A, K). \tag{7}$$

These are uniquely determined up to multipliers in F^* and are homogeneous. Moreover, there exists an invertible K-skew element u in A such that

$$p_K(p_K(b)) = (-1)^m n_K(b)^{m-2} n_A(u^{-1})\,b, \tag{8}$$

where n_A is the generic norm in A.

Proof. Let J and u be as before and define p_K by (4) and put $n_K = xp_K$. Then, as we showed above, (7) holds. Now let p_K be any polynomial map of degree $(m-1)$ of $S(A, K)$ into itself and n_K a polynomial function on $S(A, K)$ such that (7) holds. Define p_J by

$$p_J(a) = p_K(ua)\,u, \qquad a \in H(A, J), \tag{9}$$

and let $n_J(a) = n_K(ua)$. Then $p_J(a)\,a = p_K(ua)\,ua = n_K(ua) = n_J(a)$ and $ap_J(a) = ap_K(ua)\,u = u^{-1}uap_K(ua)\,u = u^{-1}n_K(ua)\,u = n_K(ua) = n_J(a)$. Hence, by Proposition 1, $p_J = p\ \#_H$ and $p_K(b) = p(u^{-1}b)^{\#_H}u^{-1}$. This proves the uniqueness assertion. Also, the homogeneity is clear form the homogeneity of n_H and $\#_H$. It remains to prove (8). Using the Zariski topology it suffices to prove this if $u^{-1}b$ is invertible or, equivalently, $n_H(u^{-1}b) \neq 0$. Then $(u^{-1}b)^{\#_H} = n_H(u^{-1}b)(u^{-1}b)^{-1}$ so $p_K(b) = (u^{-1}b)^{\#_H}u^{-1} = n_H(u^{-1}b)\,b^{-1}$. Since $(u^{-1}b)^{-1} \in H(A, J)$, $b^{-1} = (b^{-1}u)\,u^{-1} \in S(A, K)$. Hence

$$\begin{aligned} p_K(p_K(b)) &= n_H(u^{-1}b)^{m-1}\,p_K(b^{-1}) \\ &= n_H(u^{-1}b)^{m-1}\,n_H(u^{-1}b^{-1})\,b. \end{aligned} \tag{10}$$

Now $bu = u(u^{-1}b)u = -(Ju)(u^{-1}b)u$. To prove (8) we may assume that the base field is algebraically closed. Then $n_H(a)$ becomes $\mathrm{Pf}(as)$, n_A becomes the determinant det, and $J(u)$ becomes $s(u')\,s^{-1}$, where u' is the transpose of u. Hence

$$\begin{aligned} n_H(bu) &= \mathrm{Pf}(-u(u^{-1}b)(s(u')\,s^{-1}s) \\ &= (-1)^m\,\mathrm{Pf}((u(u^{-1}b)\,s)(u')) \\ &= (-1)^m \det(u)\,\mathrm{Pf}((u^{-1}b)\,s) \\ &= (-1)^m \det(u)\,n_H(u^{-1}b). \end{aligned}$$

Thus $n_H(u^{-1}b^{-1}) = n_H(bu)^{-1} = (n_H(bu))^{-1} = (-1)^m n_A(u)^{-1} n_H(u^{-1}b)^{-1}$ and hence, by (10),

$$\begin{aligned} p_K(p_K(b)) &= (-1)^m n_H(u^{-1}b)^{m-2} n_A(u)^{-1} b \\ &= (-1)^m n_K(b)^{m-2} n_A(u)^{-1} b \end{aligned}$$

as in (8). Also, $Ku = -u$ follows from $Ju = -u$ and $K = i_u J$. ∎

We call p_K and n_K which are determined up to a multiplier in F^* a *generic adjoint* and *generic norm* in $S(A, K)$. The relation (8) is called the *adjoint identity* for p_K.

Now let J' be a second involution of symplectic type in A and let $K = i_{u'} J'$, where u' is K-skew. Let p'_K and n'_K be the generic adjoint and generic norm determined as before by J'. Then $p'_K = \rho p_K$, $\rho \in F^*$. Then by the adjoint identity, $(-1)^m n'_K(b)^{m-2} n_A(u')^{-1} b = p'_K(p'_K(b)) = p'_K(\rho p_K(b)) = \rho^{m-1} p'_K(p_K(b)) = \rho^m p_K(p_K(b)) = (-1)^m \rho^m n_K(b)^{m-2} n_A(u)^{-1} b$. Since $n'_K = \rho n_K$ this gives $\rho^2 n_A(u)^{-1} = n_A(u')^{-1}$. Hence, the multiplier $n_A(u)^{-1}$ is determined up to a non-zero square in F. We note also that any invertible K-skew element u can be used in (8). For, given such a u, we can define $J = i_{u^{-1}} K$ which is an involution of symplectic type and we can use this J in the proof of Theorem 1 to obtain (8) in which $n_A(u)^{-1}$ for the given u appears. Our result shows also that for any such u and u', $n_A(u)^{-1}$ and $n_A(u')^{-1}$ differ by a multiplier in F^{*2}. We call the element $n_A(u)^{-1} F^{*2}$ of F^*/F^{*2} the *discriminant* $\delta(K)$ of the orthogonal involution K.

2. Splitting of Simple Algebras with Involution of Degree 4

Definition. An algebra with involution (A, J) is said to *split* if $A = A_1 \otimes_F A_2$ where the A_i are stabilized by J and $[A_i : F] > 1$.

In this section we consider the splitting of central simple algebras with involution of degree 4. We show first that splitting occures if J is of symplectic type.

Theorem 2. *Let A be central simple of degree 4 over F, J an involution of symplectic type in A. Then (A, J) splits.*

Proof. It suffices to show that A contains a quaternion subalgebra B stabilized by J. Then the centralizer A^B is stabilized by J and $A = B \otimes_F A^B$. There are the cases to consider: (1) $A = D$ is a division algebra, (2) $A = M_2(D)$ where D is a quaternion division algebra, and (3) $= M_4(F)$. Full details of this proof can be found in [6].

(1) If $A = D$ is a division algebra with symplectic involution J then $H(D, J) = (1 + J)D$ contains a separable quadratic subfield Q/F. Let σ be the automorphism $\neq 1_Q$ of Q/F. Then there exists an element $w \in H(D, J)$ such that $\sigma a = waw^{-1}$ for all $a \in Q$. Since $w \in H(D, J) \notin F$, $F(w)$ is quadratic over F. It follows that $B = Q[w]$ is a quaternion algebra over F stabilized by J. Full details of this proof can be found in [6].

(2) Here we consider $\mathrm{End}_D V$ where V is a two-dimensional vector space over a quaternion division algebra D. It can be seen that the symplectic involutions in $A = \mathrm{End}_D V$ are the adjoint maps relative to a non-degenerate hermitian form g on V with respect to the standard involution $a \rightsquigarrow \bar{a}$ in D. It is known that for such a form there exists a base (u_1, u_2) of V/D such that the matrix of g relative to this base has the form $\mathrm{diag}\{\alpha_1, \alpha_2\}$, $\alpha_i \in F^*$ (see, e.g., Jacobson [3, p. 153]). Then $(\mathrm{End}_D V, J) \cong (M_2(D), K)$ where

$$K: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightsquigarrow \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}^{-1}. \tag{11}$$

Now $M_2(D) = D \otimes_F M_2(F)$ where $D = \{\mathrm{diag}\{d, d\} \mid d \in D\}$ and the subalgebras D and $M_2(F)$ are stabilized by K. Hence $(M_2(D), K)$ is split.

(3) The classical result that any two invertible alternate matrices in $M_{2m}(F)$ are cogredient (see e.g. Jacobson [3, p. 161]) implies that any two $(M_{2m}(F), J)$ with symplectic J are isomorphic. The result follows by taking $(M_4(F), J) = (M_2(F) \otimes_F M_2(F), t \otimes t_s)$. ∎

We consider next involutions of orthogonal type in a central simple A of degree 4. In this case for K of orthogonal type in A we have the generic norm n_K, a homogeneous polynomial function of degree 2 on $S(A, K) = (1 - K)A$, and the generic adjoint p_K that is a homogeneous linear map of $S(A, K)$ into itself such that for any $b \in S(A, K)$ we have $bp_K(b) = n_K(b)1 = p_K(b)b$ and $p_K(p_K(b)) = n_A(u)^{-1}b$, where $Ku = -u$ and $n_A(u)^{-1}F^{*2}$ is the discriminant $\delta(K)$ of K. We now have the following.

THEOREM 3. *Let A be central simple of degree 4 with involution K of orthogonal type. Then (A, K) splits if and only if $\delta(K)$ is trivial ($= F^{*2}$).*

Proof. Suppose $(A, K) = (A_1 \otimes_F A_2, K_1 \otimes K_2)$ splits where A_i is a quaternion algebra with involution K_i. Let t_1 be the standard involution in A_1, t_2 an involution of orthogonal type in A_2. Then $t_1 \otimes t_2$ is an involution of symplectic type in $A_1 \otimes A_2$. Let u_i be an invertible element in A_i such that $K_i = i_{u_i} t_i$. Then $K = i_{u_1 \otimes u_2}(t_1 \otimes t_2)$ and hence $\delta(K) = n_A(u)^{-1}F^{*2}$ where $u = u_1 \otimes u_2$. Moreover, $n_A(u) = n_A(u_1)\, n_A(u_2)$ and $n_A(u_i) = n_{A_i}(u_i)^2$. Hence $n_A(u)$ is a square and $\delta(K)$ is trivial.

For the proof of the converse we first determine $\delta(t)$, t the the transpose involution in $A = M_4(F)$. Here $S(A, t)$ consists of the matrices of the form

$$a = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{pmatrix} \tag{12}$$

and

$$\mathrm{Pf}(a) = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}. \tag{13}$$

We now put

$$a' = \begin{pmatrix} 0 & -a_{34} & a_{24} & a_{24} & -a_{23} \\ a_{34} & 0 & -a_{14} & -a_{14} & a_{13} \\ -a_{24} & a_{14} & a_{14} & 0 & -a_{12} \\ a_{23} & -a_{13} & -a_{13} & a_{12} & 0 \end{pmatrix}. \tag{14}$$

We have that $aa' = \mathrm{Pf}(a)\,1 = a'a$ and that $a \rightsquigarrow a'$ is a linear transformation in $S(A, t)$. It follows that p_t is $a \rightsquigarrow a'$.

Now suppose K is an orthogonal involution in A such that $\delta(K) = 1$. Then we may assume that $p_K(p_K(b)) = b$ for $b \in S(A, K) = (1 - K)A$. We now define

$$S(A, K)^+ = \{a \in S(A, K) \mid p_K(a) = a\}. \tag{15}$$

Since $ap_K(a) \in F1$, we have $a^2 \in F1$ if $a \in S(A, K)^+$. Now $S(A, K)^+$ is a subspace of $S(A, K)/F$. To determine its dimensionality we extend the base field to the algebraic closure $\bar{F}$. Then we obtain $(A_{\bar{F}}, K) \cong (M_4(\bar{F}), t)$. It follows that $[S(A, K)^+ : F] = [S(M_4(\bar{F}), t)^+ : \bar{F}]$. It is clear from (12) and (14) and the fact that $p_t : a \rightsquigarrow a'$ that $S(M_4(\bar{F}), t)^+$ is the set of matrices of the form

$$a = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & -a_{14} & a_{13} \\ -a_{13} & a_{14} & 0 & -a_{12} \\ -a_{14} & -a_{13} & a_{12} & 0 \end{pmatrix}. \tag{16}$$

Hence $[S(M_4(\bar{F}), t)^+ : \bar{F}] = 3$ and $[S(A, K)^+ : F] = 3$. Now $(S(M_4(\bar{F}), t)^+$ has the base $(u = e_{14} - e_{23} + e_{32} - e_{41},\ v = e_{13} + e_{24} - e_{31} - e_{42},\ w = -e_{12} + e_{21} + e_{34} - e_{43})$ and

$$\begin{aligned} &u^2 = v^2 = w^2 = -1 \\ &uv = -vu = w,\ vw = -wv = u,\ wu = -uw = v. \end{aligned} \tag{17}$$

If char $\bar{F} \neq 2$ then $\bar{F}1 + S(M_4(\bar{F}), t)^+$ is a quaternion subalgebra of $M_4(\bar{F})$ stabilized by t. Since $(F1 + S(A, K)^+)_{\bar{F}} \cong \bar{F}1 + S(M_4(\bar{F}), t)^+$, $F1 + S(A, K)$ is a quaternion subalgebra of A. Clearly this is stabilized by K.

If Char $F = 2$, then the subalgebra of $M_4(\bar{F})$ generated by the above u, v, w is commutative and $b^2 \in \bar{F}1$ for every $b \in \bar{F}1 + \bar{F}u + \bar{F}v + \bar{F}w$. Since $(A, K)_{\bar{F}} \cong (M_4(\bar{F}), t)$ it follows that $B = F1 + S(A, K)^+$ is a commutative subalgebra of A and $b^2 \in F1$ for every $b \in S(A, K)^+$. It follows that B is is a Frobenius algebra and since $[B : F] = 4$ is the degree of A/F any derivation of B into A can be extended to an inner derivation of A (Jacobson [4]). Now B is generated by two elements x, y in $S(A, K)^+$ and we have a derivation Δ such that $\Delta x = x$, $\Delta y = 0$. Then we have an element $d \in A$ such that $dx + xd = x$, $dy + yd = 0$. Then $d^2x + xd^2 = x$, $d^2y + yd^2 = 0$, $d^2 + d \in A^B = B$ (Jacobson, [4]). Hence $(d^2 + d)^2 \in F1$. Put $f = d^2$. Then $f^2 + f = \alpha 1$ and $xf + fx = x$ or $fx = x(f + 1)$. It is readily seen that $C = F1 + Ff + Fx + Fxf$ is a quaternion subalgebra of A. Now $Kx = x$ and $(Kf)x + x(Kf) = x$. Then $(Kf + f)x = x(Kf + f)$. Also, $(Kf + f)y = y(Kf + f)$. Hence $Kf + f \in A^B = B$ and $Kf^2 + f^2 \in F1$ and $Kf^2 \in C$. Since $f^2 + f = \alpha 1$ it follows that $Kf \in C$. Hence $KC \subset C$ so C is stabilized by K. ∎

Saltman in [8] has used the preceding theorem and the concept of generic division algebra with symplectic involution to prove the following.

THEOREM 4. *Let A/F be a central simple algebra with involution of degree 4. Assume F is a Hilbertian field of characteristic $\neq 2$. Then A has an involution K such that (A, K) does not split.*

ACKNOWLEDGMENTS

I am indebted to Adrian Wadsworth for a number of comments on an earlier version of this paper that led to improvements of the results and exposition. I am also indebted to the referee for pointing out some errors.

REFERENCES

1. A. A. ALBERT, "Structure of Algebras," AMS Colloq. Publications, 1939.
2. S. A. AMITSUR, L. H. ROWEN, AND J. P. TIGNOL, Division algebras of degree 4 and 8 with involution, *Israel J. Math.* **33** (1974), 133–148.
3. N. JACOBSON, "Lectures in Abstract Algebra," Orig. ed. van Nostrand, New York, 1953; Springer-Verlag, New York/Berlin, 1975.
4. N. JACOBSON, Generation of separable and central algebras, *J. Math. Pures Appl.* **36** (1957), 217–227.

5. N. JACOBSON, Generic norms I, *in* "Proceed. Conference in Algebra, Novosibirsk, 1989."
6. N. JACOBSON AND D. SALTMAN, "Finite Dimensional Division Algebras," Grundlehren der Mathematischen Wissenschaften, Springer, Berlin/New York, to appear.
7. M. A. KNUS, R. PARIMALA, AND R. SRIDHARAN, Involutions on rank 16 central simple algebras, *J. Indian Math. Soc.*, to appear.
8. D. SALTMAN, A note on generic division algebras, to appear.